Besieged privacy in social networking services

Shujun Dong*

China University of Political Science and Law,
Xitucheng Road 25, Haidian District,
Beijing, 100088, China
Email: fwb196886@163.com
*Corresponding author

Xingan Li

School of Governance, Law and Society,
Tallinn University,
Narva MNT 29, Tallinn, 10120, Estonia
Email: xingan.li@tlu.ee

Abstract: The aim of current paper is to investigate the risks of illegal use of personal information brought about by the social networking services (SNSs). The principal theme considered in this paper is that, the SNSs, in front of both conventional and unconventional offenders, have induced worry about unlawful access to accounts, disclosure and infringement of privacy, as well as misuse and abuse of anonymity. On the grounds that there are more sensitive information and clues and traces to daily activities and movements, it is uncomplicated for possible malefactors to select possible victims of varieties of offences. The article concluded that social networking services facilitated both traditional and untraditional privacy-related crimes with both traditional and untraditional scheme, and reviewed alternative solutions to privacy protection and their concomitant dilemmas. An international initiative might be more realistic for coordinating national divergences.

Keywords: social networking services; SNSs; offences against privacy; offences against property; anonymity; real-name system.

Reference to this paper should be made as follows: Dong, S. and Li, X. (2016) 'Besieged privacy in social networking services', *Int. J. Electronic Security and Digital Forensics*, Vol. 8, No. 3, pp.224–233.

Biographical notes: Shujun Dong is an Associate Professor at China University of Political Science and Law, China. She received her LLB, LLM, and LLD degrees. Her research interests are economic crime, cybercrime, and theory and practice of criminal penalty.

Xingan Li is an Associate Professor at Tallinn University, School of Governance, Law and Society, Estonia. He received his LLB, LLM, LLD and PhD in Computer Sciences. He was an Associate Professor at Inner Mongolia University, China; an Attorney at Fayuan Law Firm, China; a visiting scholar at Kyushu University, Japan; and a researcher at University of Turku and University of Tampere, Finland. His research interests are cybersecurity, cybercrime and social order in cyberspace, application of data mining methods in the research of crime, and law and digital technology.

1 Introduction

The development of information technology and the pervasive use of the internet have not only divided but also integrated the society. More and more people are living a double life, online and offline. More and more online life is related to social networking services (SNSs). The users' involvement and participation in SNSs mean both intimate and alien penetration into their being, life, soul, ego, safety, privacy, and security. In a previous research, it was concluded that the information systems could be target, tool, media, route, place, and means of crimes and can be used in preparation for other offences [Li, (2008), p.131]. This can well be applied to the new case of the SNSs.

The purpose and thus emphasis of this article is to explore into the features of SNSs in the sense of privacy protection, that is to say, to study how SNSs facilitate potential perpetration of privacy-related offences as well as victimisation. Typical features that are not so closely relevant will not be considered. Therefore, this article will not give exhaustive consideration of features of the SNSs that are otherwise significant. They are tailored in the way that they serve the content of this article. It is specifically important to mention that, there are features of the SNSs that are possible to enhance social welfare, or to play important roles in helping to prevent, deter or detect offences one way or the other. Limited to the content of this article, these 'constructive' features are temporarily forgotten here. Other interested study may be concentrated on the deterrence effect of the SNSs. That will be another potential valuable research.

Following this introduction, the next sections will present known fields that can be seen as risky or destructive aspects of the SNSs in facilitating privacy-related offences and causing victimisation. The last section will conclude the article with discussions on the findings of the study.

2 SNSs and related offences on the rise

Social order in cyberspace has been a central concern of law enforcement in recent years (Li, 2009). Adding to existing complicacy is the emergence of fresh facets of the SNSs. The terms, SNSs, social networking sites, or social network sites, all abbreviated as SNSs, can be used interchangeably to denote the similar (if not the same) phenomena, which are presently very popular and well known in the information society. People named and defined them in various ways. Presently, SNSs are not limited to those provided by websites. Rather, they can be also served via computer or mobile applications. Therefore, the most feasible term might be SNSs. Nevertheless, here we will neither discuss in detail about the divergence of these terms and their definitions, nor the divergence of actual services. This article only adopts a convenient definition: SNSs are "web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system" (Boyd and Ellison, 2007). According to the Federal Bureau of Investigation, social networking sites are internet-based services that allow people to communicate and share information with a group (FBI, 2015).

According to such a definition, SNSs can be provided by websites, or computer or mobile applications, sometimes by both. For example, QQ has both an independent application and a website contributing to different parts of the networking services. From

the languages of the services, the SNSs provided in English and, simultaneously, in many other languages can be thought as universally accepted services, such as MySpace, Facebook, LinkedIn, Twitter, Google+, etc. Some of the services might be only available in a limited number of languages, such as QQ (primarily in Chinese, but one basic version also in English), WeChat (in simplified and traditional Chinese, English, and German), etc.

Due to the nature of such websites and applications, these services are not space-specific. However, in some specific cases, certain services do not reach users in certain countries. For example, FaceBook, MySpace, Twitter, Google+, and many other services are normally inaccessible by users in mainland China due to the strict censorship and filtering system imposed on inward and inside contents and services. Popular SNSs accessible in China are LinkedIn and Tumblr, as well as ResearchGate, which is sometimes taken as SNSs for researchers. While those inside contents and services will not be permitted to exist for a long time, those inward ones can be stopped by the potential Great Firewall.[1] Anyway, compared with North Korean network, the Chinese one is already open enough. Despite such limits, in countries like China, other SNSs are still broadly available due to the fact that domestic services are permitted under the premise of submission to the official regulations.[2] It indicates that just the same phenomena taking place among users, misusers and abusers in one geographic location of the world can take place among their counterparts in another geographic location as well.

SNSs involve an increasing number of people all over the world. Globally 3.2 billion people will use the internet by the end of 2015 [ITU, (2015), p.1].[3] By the end of 2015, there will be more than 7 billion mobile cellular subscriptions, corresponding to a penetration rate of 97% [ITU, (2015), p.2]. While the number of users of the SNSs is not available, it was estimated that among internet users, about 74% of online adults use social networking sites (Pew Research Center, 2015). We do not further confirm or suspect the accuracy of these figures, but the accuracy of these figures is not so important for our study. That's sufficient that these figures represent a roughly depictive position and tendency in the transformation of social lives. However, they provide with us an important indicator on the scale of the SNSs and their influence on many lives of our society.

With the scale of using the SNSs enlarged, SNS-related offences are also increasing. It was reported that, in the UK in 2011, about 12,300 alleged offences, including murder, rape, child sex offences, assault, kidnap, death threats, witness intimidation and fraud, involved the popular SNS FaceBook were reported to the police (Doyle, 2012). According to Chinese official media, People' Daily (He and Ma, 2014), about 85 cases, exploiting popular Chinese SNS WeChat, were accepted for trial in courts of five cities in Guangdong Province alone during 2012–2013. Presently, cybercriminals are also turning to the SNSs. It was estimated that 81 percent of internet-initiated crime involves SNSs, mainly Facebook and Twitter, which provide ideal resource for criminals to dig up private data from unsuspecting individuals (Pew Research Center, 2015). Yet worse, offline offences, such as burglars, sex offenders and other crooks are also take advantage of the SNSs. Among them, 78 percent of burglars confessed that they exploited social media to seek out their victims *(ibid.*).

Apparently, as the SNSs provide users with many new opportunities for communication and cooperation, they also bring about risks and dangers, probably victimising their life, health and property.

3 Privacy concerns in the SNSs

Privacy has always been a critical element when getting connected to the computer network, and today, when getting connected to the digital social network. People take privacy differently. Disputation about to what extent privacy should be protected has always been greatly divided between different interest groups and cultural contexts. This article does not deal with different arguments, but will go through how the features of behaviours of the users of SNSs can involve privacy concerns.

Traditionally, social network can also grow bigger and bigger with relatives, friends and colleagues as intermediaries. However, imagine, traditional friend's friend could get connected with help of the direct friend. But someone's friend's friend would face more difficulties in getting connected, not to mention friend's accurate information being obtained by friend's friend through mere social interaction. It did simply not take place so often.

However, users of present SNSs and their friends' friends are put into closer relationship than in the traditional case. Usually, users' information is available to 'friends' within several layers of relationship. Sometimes, users' profiles are completely public, while traditionally, such information was only available to a small circle of relatives, neighbours or close friends, existed only in one's official archives, and was confidential. On the SNSs, we can say that, everywhere and every moment, there are bulletin boards, where users' traditionally private information is now publicised.

The SNSs themselves greatly changed the old privacy ideas. In meat society, to give a full picture of somebody, it took a long time, hard efforts, and much energy. In cyberspace, to depict someone who is a frequent user of SNSs, takes just some clicks of the computer mouse: many aspects of demographic information, physical condition, family life, education background, work experience, hobbies, achievements, honours and awards, daily activities, consumption habit, financial situation, category of housing, brand of car, travel time and destinations, psychological state and quality, political views, pieces of information about relatives, as well as 'friends' in the social network.

Limited to available resources, conventional media were limited to report and record public events and public figures. A major part of the general public used to be beyond the coverage of conventional media. However, today's SNSs make it possible for all the users to form a media atmosphere, where they are both correspondents and audience, as it is put in Chinese users, 'zi meiti' (self-media). Every one can be her/his own reporter and be willing to publicise her/his own dynamic information, and every one at the same time is other users' audience and be willing to listen, read, follow, enjoy, and interact. While users voluntarily or inadvertently publish a great amount of sensitive information on popular SNSs with the intent provide news or other updates to their audience for informational or social purposes, some of this information may be misappropriated and used for the benefit of criminal activity [UNODC, (2012), p.11].

In a word, both the speed and the range of information dissemination have been highly improved than the pre-SNS time. The controllability of the self-media becomes more difficult than traditional media. As FBI (2015) put it:

> "Once information is posted to a social networking site, it is no longer private. The more information you post, the more vulnerable you may become. Even when using high security settings, friends or websites may inadvertently leak your information."

Once private information was disseminated, it will be soon spread to all over the internet, theoretically, not spatial and linguistic borders.

What makes privacy more vulnerable is that, history of the SNSs proved that most SNS users have been willing to share their own information (sometimes privacy) in online areas that are accessible to one or more layers of their relatives, friends, and colleagues, or even in public online areas, that is to say, such information is accessible to users that are completely not connected to the information disseminators or even to non-users. Such behaviour mode can involve the motivation of self-disclosure, via which privacy is transformed into public (available) information. The exploitation of public available personal information in illegal activities can be one of the drawbacks that characterises the SNSs.

Besides active disclosure (share) due to lack the sense of security, safety and self-protection, passive disclosure (divulgence) is another aspect of privacy concern that is frequently accompanying the SNSs. Through unauthorised access of various kinds, private information is also possible to suffer thefts by either connected or unconnected users. This kind of privacy infringement is quite often accompanied by unauthorised access. Active and passive disclosure combined makes privacy more vulnerable than ever before. Considering the content that can be revealed from the SNSs, adding such vulnerability, the criminal exploitation of personal information via the SNSs is expanding beyond the control of traditional methods, jurisdictions, and enforceability.

As a result, large amount of user data, such as personal information, images, audios and videos continue to rapidly fall into the hands of authorities, strangers, recruiters, and even the public [Ai et al., (2009), p 278]. Due to the connecting nature of the SNSs, when users share personal information, they and their associates are open to attacks (FBI, 2015). The more information shared, the more probably someone might masquerade as the users and trick one of their friends into sharing private data, downloading malware, or providing access to constrained sites (FBI 2015).

At the SNS provider layer, the SNSs do not make users aware of the dangers of divulging their personal information; privacy tools in SNSs are not flexible enough to protect user data; and the users cannot control what others may reveal about them [Ai et al., (2009), pp.272–274]. In one word, many weak aspects of the SNSs in protecting privacy add up and form a dangerous environment where privacy is left vulnerable.

4 Unauthorised access to SNS accounts

In traditional sense, pure residential trespass, without causing further damages, can already constitute a criminal offence according criminal law in many countries.[4] When these countries started tackling digital trespassing, many of them criminalised and penalised acts such as unauthorised access to information systems, information resources, and account information.

Since the beginning of the phenomena of unauthorised access taking place, there has been the differentiation between benign hacking and harmful hacking. Benign hacking was basically pure unauthorised access neither making further unauthorised use of any information resources nor causing any further damages. Harmful hacking of the SNSs can exploit the access to commit other offences, such as stealing credit information, harassing legitimate users, defrauding persons in the users' social network, acquiring

competition advantage, obtaining monetary benefits and other assets, threatening public security, and even launching terrorist activities.

Nevertheless, it must be noted that unauthorised access to the personal SNSs information can sometimes more disastrous to users as well as other members in their digital social network. Due to the fact that there are more demographic information and/or identity information, financial and consumption information, and clues and traces to daily activities and movements, it is easier for potential perpetrators to choose potential victims of many kinds of offences, to track and locate them, to stalk them, to lure and to trap them, and in some extreme cases to abduct and to kill them.

5 Dilemmas in anonymity system

In protecting SNS-related privacy, there are many different possible ways. From states' legal requirements, we can divide such protective projects into two big categories. One is anonymity system, and the other is real-name system. Both ways are in actual fact ideal models. The following will look at their pros and cons.

Anonymity is the most disputable topic covering a broad range of legal aspects. Human rights organisations usually argue for anonymity, because under real-name system, users' authentic personal information could be directly collected and it can render direct exploitation by Governments, corporations, criminals and pranksters to interfere with the rights to freedom of opinion and expression through online censorship, mass and targeted surveillance and data collection, digital attacks on civil society and repression resulting from online expression [Kaye, (2015), p.3]. From the viewpoint of freedom of expression, it is surely important to protect users from illegal activities. This is also important for maintain privacy.

> "Encryption and anonymity, today's leading vehicles for online security, provide individuals with a means to protect their privacy, empowering them to browse, read, develop and share opinions and information without interference and enabling journalists, civil society organizations, members of ethnic or religious groups, those persecuted because of their sexual orientation or gender identity, activists, scholars, artists and others to exercise the rights to freedom of opinion and expression." (*ibid.*)
>
> "The use of encryption and anonymity tools and better digital literacy should be encouraged." (*ibid.* p. 21)

However, online anonymity does not always play a constructive role in maintaining social order. Online anonymity has been discussed for a long time. Whereas privacy is at high risk, anonymity causes broad concerns. From law enforcement standpoint, the anonymity of cyberspace makes identity tracing a significant quandary which poses obstacles in law enforcement. It has been found that cyber anonymity has critical impacts on criminal motivation, and the phenomena of victimisation, and should be tackled on different layers including technology and law enforcement (Li, 2014). The function of the internet as an approach of communications and with an elevated anonymity of interaction repeatedly entraps the victims into unforeseeable trouble. In numerous criminal cases, stalkers and murderers discover, chase, allure, and terrorise victims in the course of the communication and interaction of a variety of internet services, typically anonymously. In addition, the internet, and particularly, SNSs have been reportedly used by international terrorism (Weisburd, 2011; UNODC, 2012).

Today, communicating anonymously between direct SNS 'friends' is not fully the case in the SNSs. However, due to the nature of most SNSs, indirect connections can maintain anonymity from the beginning to the end. With the increase of layers of connections, the degree of anonymity becomes higher and higher. For example, a user's friend or associate in the SNSs, is usually in a position that they know each other very well. They can easily acquire each other's personal information, both offline and online. In an outer cycle, 'friend's friend' or 'associate's associate' is that who can have access to the user's online information, but does not have first-hand offline information. The outer the cycle, the less the information acquired. Finally, friends or associates in several outer cycles could in factual fact be anonymous with each other. While some users use their own real name and publicise their authentic information, others may keep some extent of privacy or anonymity among friends or associates.

Connections in online social network, like that in offline networks, can exploit the anonymous self to infringe the real-name others. This cyber society has exactly the same differentiation between good and evil. It has been proved that many of the traditional offline deviances had been transplanted to the online body of the society, called cyberspace. It has been proved that in cyberspace, there have occurred many other deviances that were not existing offline before. It has also been proved that more and fresher kinds of online deviances were emerging in a rapid step. Therefore, we do not expect that all the nearly anonymous 'friends or associates' are free from devoted themselves in various kinds of deviances. In fact, many of them have already been motivated by greedy, hatred and passion to target their SNS friends or associates.

In traditional society, as a proverb says, "a friend in need is a friend indeed". But today, a, anonymous SNS 'friend' of many cycles outer can unfortunately be a 'friend' in need of your property, your money, and your privacy. Cyber anonymity has deep impact on occurrence of cybercrime, mostly reducing the potential likelihood of detection and thus its costs (Li, 2014). In fact, anonymity may to some extent encourage potential perpetrators to take the risk. On the other hand, victims may lose opportunities to make judgment on whether or not it is of their interest to interact with hidden perpetrators. Once crime occurs, anonymity further hinders law enforcement from detecting and investigating.

6 Dilemma in real name system

The second alternative practise is real-name system, which means that identity of all users is required to be verified before their account can be activated. The principle of such a practice is that if and only if all users have verified identity, legitimate users can identify their real connections. If some users registered with authentic personal information, while other users registered with fake personal information can have access to authentic users' information, users with authentic information can no longer enjoy their privacy. It is very difficult to protect real users' privacy from potential infringement by fake users.

In China, real-name system has been implemented in many online services. One of the most recent regulations are "Internet User Account Name Management Regulations" promulgated by China National Internet Information Office and took effect on 1 March 2015. "Internet user account names as mentioned in these Regulations, refers to the account names of bodies or individuals registered or used in blogs, microblogs, instant

communication tools, forums posting bars, posting comments and other such Internet information services" (Internet User Account Name Management Regulations, Article 2).

For over two decades, Chinese law already required people to open bank accounts by using real names verified with identification card. In managing the SNSs, real-name system has been strictly implemented. Article 5 of the above mentioned regulations requires internet information service providers to abide by the principle of "real name backstage, voluntary choice front stage", that is to say, demanding internet information service users to register accounts after undergoing real identity information authentication. For example, to register a personal WeChat platform that can be used to publish personal texts, photos, audios and videos, a user must bind a personal credit card with the WeChat account. Although to register a WeChat account is far easier or even anonymously, a WeChat platform account must be verified with the user's bank information.[5]

The realisation of real-name system for all users is an ideal way to protect all users' privacy against any fake users' infringement. However, the risks also increase with users with authentic registration information. If all users use random information, either authentic or fake, privacy are not so clearly revealed. However, if most users use authentic information, only potential perpetrators use fake information, real users are taking much greater risks of disclosure their information to uninvited guests. Therefore, real-name system is an ideal mechanism, but not a perfect one.

At the international level, use of the internet in counter-crime and counter terrorism inevitably involves the surveillance and collection of information relating to suspects [UNODC, (2012), p.14]. Users' personal information about their identity and personal life should be protected from illegal infringement. Conditions of lawful interference of privacy must be detailed in domestic laws, while any abuse should be avoided through feasible safeguards (ibid.).

Of course, when we talk about real-name system in China, we must consider the purpose of such a system. Generally speaking, first of all, it was established for prevent the user from publish anonymous political speech, prevent the user from abusing the services, and once such abuse occurs, the perpetrator can be conveniently detected, investigated and identified. By taking the risks of victimising users' privacy, the state organs can well control and grasp the unfavourable speeches and activities, and to some extent, well protect many of the service users as well. But anyway, this is a system full of dilemmas.

7 Conclusions

SNSs, as one of the central activities that contemporary people are involved in, have transformed modern social lives. It is natural that the conventional social phenomena advance toward the new extended space, cyberspace. As the SNSs provide users with many new opportunities for communication and cooperation, they also bring about risks and dangers, probably victimising their life, health and property.

Privacy has always been a critical element when getting connected to the computer network, and today, when getting connected to the digital social network. Besides active disclosure (share) due to lack the sense of security, safety and self-protection, passive disclosure (divulgence) is another aspect of privacy concern that is frequently accompanying the SNSs. SNSs, besieged by both offline and online offences, have

incurred concerns on unauthorised access to accounts, disclosure and infringement of privacy, as well as misuse and abuse of anonymity. SNSs facilitated both traditional and new privacy-related crimes with both traditional and new methods.

In protecting SNS-related privacy, there are many different possible ways. From states' legal requirements, we can divide such protective projects into two big categories. One is anonymity system, and the other is real-name system. In fact, these two categories of protective projects are always associated with dilemmas: to protect and to be exploited. This situation is further perplexed by the fact that there are widely divergent socio-cultural traditions and politico-legal concepts.

Under such circumstances, it is not possible to coordinate transnational regulations depending on domestic laws of individual countries. More than ever, international initiative is a shortcut towards better privacy protection and more successful law enforcement. However, whether it should be anonymity or real-name system, such an international initiative still needs practical test.

References

Ai, H., Maiga, A. and Aimeur, E. (2009) 'Privacy protection issues in social networking sites', *Proceedings of The 7th IEEE/ACS International Conference on Computer Systems and Applications, AICCSA 2009*, 10–13 May, Rabat, Morocco, doi: 10.1109/AICCSA.2009.5069336.

Boyd, D. and Ellison, N. (2007) 'Social network sites: definition, history, and scholarship', *Journal of Computer-Mediated Communication*, Vol. 13, No. 1, Article 11, pp.210–230.

China National Internet Information Office (2015) *Internet User Account Name Management Regulations*, China National Internet Information Office, Beijing.

Doyle, J. (2012) *A Facebook Crime Every 40 Minutes: From Killings to Grooming as 12,300 Cases Are Linked to the Site* [online] http://www.dailymail.co.uk/news/article-2154624/A-Facebook-crime-40-minutes-12-300-cases-linked-site.html (accessed 30 May 2015).

FBI (The Federal Bureau of Investigation) (2015) *Internet Social Networking Risks* [online] http://www.fbi.gov/about-us/investigate/counterintelligence/internet-social-networking-risks (accessed 30 May 2015).

He, L. and Ma, Y. (2014) 'Liyong Weixin Fanzui Anjian Pinfa, Guangdong Fayuan Jianyi SHiming Renzheng', *People's Daily*, 11 August, p.4.

International Telecommunication Union (ITU) (2015) *ICT Facts & Figures*, International Telecommunication Union, Switzerland.

Kaye, D. (2015) 'Report of the special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression', *The United Nations Human Rights Council 29th Session*, Geneva, Austria.

Li, X. (2008) *Cybercrime and Deterrence: Networking Legal Systems in the Networked Information Society*, Doctoral dissertation, University of Turku, Faculty of Law, Turku, Finland.

Li, X. (2009) *Social Order in Cyberspace*, ICFAI University Press, Hyderabad, India.

Li, X. (2014) 'Phenomenal exploration into impact of anonymity on law and order in cyberspace', *Kriminologija i socijalna integracija*, Vol. 22, No. 2, pp.102–123.

Pew Research Center (2015) *Social Networking Fact Sheet* [online] http://www.pewinternet.org/fact-sheets/social-networking-fact-sheet/ (accessed 30 May 2015).

United Nations Office on Drugs and Crime (UNODC) (2012) *The Use of the Internet for Terrorist Purposes*, United Nations Office on Drugs and Crime, Vienna.

Weisburd, A.A. (2011) *Jihadist Use of Social Media: How to Prevent Terrorism and Preserve Innovation*, 6 December, testimony of A. Aaron Weisburd, Director, Society for Internet Research, before the United States House of Representatives Committee on Homeland Security, Subcommittee on Counterterrorism and Intelligence.

Notes

1 The original use and its strict definition were not recorded in literature. But it is usually used to denote the strict censorship and filtering system implemented by the Chinese government on computer network systems.

2 For the purpose of writing this article, the authors specifically investigated the accessibility of these SNSs. Three academic colleagues from different cities within mainland China tested and gave the authors their feedback on 31 May–2 June, 2015.

3 According to the website, Internetlivestats, "current internet user population estimates are delivered by Worldometers' RTS algorithm, which processes data elaborated through statistical analysis after being collected from the following sources: International Telecommunication Union (ITU) – United Nations specialized agency for information and communication technologies and the official source for global ICT statistics, The World in 2014: ICT Facts and Figures – ITU, Measuring the Information Society - ITU MIS Report 2013, Internet Users Data - World Bank Group, The World Factbook: Internet Users – U.S. Central Intelligence Agency, United Nations Population Division - U.N. Department of Economic and Social Affairs".

4 In traditional law, trespass, with a very broad range of acts, could breach either criminal law or tort law, infringing rights of the person, movable property or real estate.

5 This requirement can be tested by visiting the platform homepage https://mp.weixin.qq.com/.